Method for Implementing Access Restriction of Mobile Networks

Field of the Technology

The present invention relates to mobile communication technologies. More particularly, the invention relates to a method for implementing access restriction of mobile networks.

Background of the Invention

Nowadays, in the Global System of Mobile (GSM) network, mobile subscribers are able to roam among GSM networks of different operators, and the GSM networks can also implement access restriction to the mobile subscribers. Methods for implementing the access restriction in the GSM networks are very mature. One of the methods can obtain a Public Land Mobile Network (PLMN) number of a home GSM network of the subscriber by analyzing User Identifiers such as International Mobile Subscriber Identity (IMSI) or Mobile Station Integrated Services Digital Network (MSISDN) number. Since different operators have different PLMN numbers of their networks, this method can determine and obtain the home GSM network of the subscriber by the obtained PLMN number, accordingly, the corresponding access restriction can be implemented to the subscriber according to the home GSM network of the subscriber. A detailed implementation procedure includes:

If no roaming permission contract is subscribed between GSM networks of two operators, when a Mobile Station (MS) of a first GSM network roams into a second GSM network, the MS will initiate a Location Registration Request to the second GSM network. The second GSM network obtains the PLMN number of the home network of the MS by analyzing the user identifier of the MS, and then determines that the home GSM network of the MS is the first GSM network. Therefore, the

second GSM network returns a Location Registration Reject Message, with a reason value of "the PLMN number is not permitted" to the MS. The MS writes the PLMN number in the reason value of the message in a list of "PLMN forbidden to access" in the Subscriber Identity Module (SIM) of the MS after receiving the reject message, wherein the list will still be saved in the SIM card when the MS is shut down or the SIM card is taken out of the MS; the MS can implement access restrictions by the list of "PLMN forbidden to access". When the MS operates in a automatic PLMN network selection mode, if the PLMN number of the selected network is in the list of "PLMN forbidden to access", the MS will not initiate the Location Register Request to the GSM network corresponding to the PLMN number, thereby the access restriction is implemented automatically; when the MS operates in a manual PLMN network selection mode, if the MS successfully accesses to a certain PLMN network, the MS will determine whether the PLMN number of the network exists in the list of "PLMN forbidden to access", if it exists, the PLMN number will be deleted from the list of "PLMN forbidden to access", so that the MS is able to initiate the Location Register Request to the PLMN network in the automatic PLMN network selection mode. By the list of "PLMN forbidden to access", the method can automatically forbid the MS to initiate the Location Register Request to the PLMN network which is forbidden to access, so the demand for access restriction is satisfied.

However, with the emergence of the 3rd Generation (3G) networks, such as Wideband Code Division Multiple Access (WCDMA), the above-mentioned method cannot satisfy the demand of access restriction. For instance, some operators may simultaneously have a GSM network and a WCDMA network, and the GSM network and the WCDMA network can respectively have their own PLMN numbers or share the same PLMN number. If they share one PLMN number, the GSM network and the WCDMA network cannot be differentiated according to the PLMN number, therefore it is impossible to implement the access restriction of the GSM network or the WCDMA network. Similarly, as for networks of other types, the above-mentioned problem still exists.

Summary of the Invention

In view of the above, the present invention is to provide a method for implementing access restriction of mobile networks; the method can differentiate types of networks sharing one Public Land Mobile Network (PLMN) number and implement access restriction upon the networks of different types.

The present invention provides a method for implementing access restriction of mobile networks, and the method includes the steps of:

a Mobile Station (MS) inquiries a list of forbidden PLMNs and access technology identifiers, which is saved by the MS, when selecting the PLMN network;

the MS determines whether the selected PLMN network and the access technology exist in the list of forbidden PLMNs and access technology identifiers, if they exist, the MS will not send a Location Updating Request to a Mobile Switching Center/Serving GPRS Support Node (MSC/SGSN) of a Core Network; otherwise, the MS will send the Location Updating Request to the MSC/SGSN in order to access to the network.

It can be seen that, access restriction is implemented with the information in the list of forbidden PLMNs and access technology identifiers stored in the Subscriber Identity Module/Universal Mobile Telecommunication System SIM (SIM/USIM), thereby the requirements of network access restriction upon various access technologies are satisfied. The present invention makes it possible to implement the access restrictions upon different types of access networks by using different restriction rules. Furthermore, during the process of implementing the access restriction, the modification to the existing networks and user terminals is small, thus the method is easy to implement and can satisfy demands on access restriction of the operators.

3

Brief Description of the Drawings

Figure 1 is a flow chart for implementing an embodiment of the present invention.

Figure 2 is a flow chart illustrating the procedure of generating the list of forbidden PLMNs and access technology identifiers.

Figure 3 is a schematic diagram illustrating the 5n-1st byte of the access restriction rule data in an embodiment of the present invention.

Figure 4 is a schematic diagram illustrating the 5nth byte of the access restriction rule data in an embodiment of the present invention.

Detailed Description of the Invention

A method for implementing the access restriction of mobile networks is provided. Access technology identifiers are added in the list of "PLMN forbidden to access", and the access restriction is implemented by using the PLMN numbers and the access technology identifiers in the list, therefore satisfying the demand of the access restriction upon different types of networks.

The embodiments of the present invention will be described in detail hereinafter with reference to the accompanying drawings.

As shown in Figure 1, an embodiment of the present invention is implemented through the following steps when the MS selects to access a PLMN access network:

Step 101: the MS inquires about the list of forbidden PLMNs and access technology identifiers, which is saved in the SIM/USIM of the MS, when entering an automatic PLMN network selection mode.

Step 102: the MS determines whether the automatically selected PLMN network and the access technology exist in the list of forbidden PLMNs and access technology identifiers. If they exist, it represents that the selected PLMN access network is forbidden to access, then the MS will not send a Location Updating Request to an Mobile Switching Center/Serving GPRS Support Node (MSC/SGSN) of the Core Network, and ends the procedure; otherwise, it represents that the selected PLMN access network is allowed to access, executing step 103;

Step 103: the MS sends the Location Updating Request to the MSC/SGSN through the selected PLMN access network, and accomplishes the roaming of the MS.

In an embodiment of the present invention, as shown in Figure 2, the list of forbidden PLMNs and access technology identifiers mentioned in step 101 and step 102 is generated through the following steps:

Step 201: the MS sends the Location Updating Request to the MSC/SGSN through the access network;

Step 202: if the MSC/SGSN determines not to permit the subscriber to access the network through the current access network, it returns a Location Updating Reject Message to the MS, with the reason value in the Location Updating Reject message. The reason value can be one of the "PLMN not permitted" and the "PLMN current access technology not permitted" according to different location updating rejection reasons. The reason value of "PLMN current access technology not permitted" is a newly-added reason value in the Location Updating Reject Message for implementing the embodiment of the present invention;

Step 203: the MS records the PLMN number of the access network and the access technology identifier which are forbidden to access in the list of forbidden PLMNs and access technology identifiers, which is stored in the SIM/USIM of the MS, according to the reason value in the Location Updating Reject message. The list

of forbidden PLMNs and access technology identifiers is an expanded list from the list of "PLMN forbidden to access" in the prior art, Table 1 is an embodiment for implementing the list.

Table 1

1 to 3	1st PLMN	3 bytes
4 to 5	1st PLMN Access technology identifier	2 bytes
6 to 8	2nd PLMN	3 bytes
9 to 10	2nd PLMN Access technology identifier	2 bytes
:	:	
(5n-4) to (5n-2)	Nth PLMN	3 bytes
(5n-1) to 5n	Nth PLMN Access technology identifier	2 bytes

Referring to Table 1, which includes the PLMN numbers and the access technology identifiers, one PLMN number and one corresponding access technology identifier form one group of access restriction rule data in the list express one PLMN number and its access technology forbidden to access. The list includes at least one group of access restriction rule data, wherein, each group of the access restriction rule data occupies five bytes. Each the first three bytes is used for storing the PLMN number. Each the forth and the fifth bytes is respectively used for storing the access technology identifier. In each byte used for storing technology identifiers, each of the 8bits of each byte represents one kind of access technology, and the bit value 0 represents the access technology is permitted to access; while the bit value 1 represents the access technology is forbidden to access. As shown in Figure 3 and Figure 4, taking the 5n-1st byte and the 5nth byte shown in Table 1 as example, in the implementation of the 5n-1st byte shown in Figure 3, the 8th bit of this byte represents a UMTS Terrestrial Radio Access Network (UTRAN) (WCDMA wireless access technology), and if this bit is 1, it indicates that the WCDMA wireless access technology is a forbidden access technology; if this bit is 0, it indicates that the

6

WCDMA wireless access technology is a permitted access technology; the other 7 bits of this byte are RFU, reserved for future access technologies. in the implementation of the 5nth byte shown in Figure 4, the 8th bit of this byte represents the GSM wireless access technology, if this bit is 1, it indicates that the GSM wireless access technology is a forbidden access technology, and if this bit is 0, it indicates that GSM wireless access technology is a permitted access technology; the 7th bit of this byte represents a GSM COMPACT wireless access technology, if this bit is 1, it indicates that the GSM COMPACT wireless access technology is a forbidden access technology, if this bit is 0, it indicates that the GSM COMPACT wireless access technology is a permitted access technology; the other 6 bits are RFU, reserved for future access technologies;

In Step 203, the step of the MS recording the PLMN number of the access network and the access technology identifier which are forbidden to access in the list of forbidden PLMNs and access technology identifiers further includes:

the MS analyzes the reason value in the Location Updating Reject Message after receiving the Location Updating Reject message from the MSC/SGSN, if the reason value is "current access technology of PLMN is not permitted", the MS records the PLMN number of the access network that the MS is located currently, and the access technology identifier in the list of forbidden PLMNs and access technology identifiers. If the reason value is "PLMN is not permitted", it is indicated that all the access technologies in the access network represented by the PLMN number are not permitted to access. Under such circumstances, the MS records the PLMN number in the list of forbidden PLMNs and access technology identifiers. All the access technology identifiers corresponding to the PLMN number in the list are set as 1, which is used for indicating that any type of access network is forbidden to access to the PLMN network;

The content of the list of forbidden PLMNs and access technology identifiers also can be modified, and the modification is implemented as follows:

if the MS successfully access to a certain PLMN network through one access technology in a manual PLMN network selection mode, the MS determines whether the PLMN number of the accessed network and corresponding access technology identifier exist in the list of forbidden PLMNs and access technology identifiers saved by the MS. If they exist in the list, the MS sets the bit corresponding to the access technology in the access technology identifier corresponding to the PLMN number as 0, so as to delete the access technology identifier from the list of forbidden PLMNs and access technology identifiers. After setting the bit as 0, the MS checks whether all the bits of each byte in the access technology identifier corresponding to the PLMN number are 0. If they are all 0, it indicates that all the access technologies corresponding to the PLMN number are all access technologies permitted to access, therefore deleting the PLMN number and the corresponding access technology identifiers, i.e. one group of the access restriction rule data of 5-byte, from the list of forbidden PLMNs and access technology identifiers; otherwise, this group of access restriction rule data can be reserved.

The above-mentioned embodiments are only embodiments for implementing the access restriction in the GSM network and the WCDMA network. The present invention also can be applied to other networks such as WLAN、 Bluetooth, etc., corresponding implementation is similar to those mentioned above.

The above-mentioned embodiments are only the preferred embodiments of the present invention, and not used to confine the protection scope of the present invention, it is apparent that various changes, substitution of equivalent parts and improvements can be made within the scope of the present invention as defined by the appended claims.